Data Expiration, Let the User Decide: Proposed Legislation for Online User-Generated Content

By KAREN MAJOVSKI*

Introduction

THE INTERNET REMEMBERS ALL, and for some individuals this comes at a cost. Take the story of twenty-five-year-old, soon-to-be schoolteacher Stacy Snyder, whose university denied her a teaching certificate because of a picture she posted to her MySpace page.[1] The photo depicted the student teacher wearing a pirate hat while holding a plastic cup with the caption, "drunken pirate."[2] When university officials learned about the picture, they determined it was improper for a student teacher to represent herself in that manner.[3] As a result, the university denied Ms. Snyder a teaching certificate.[4]

Jean-Sun Hannah Ahn, a college student, also fell victim to the Internet's perfect digital memory in December 2011.[5] Before she en-

* J.D. Candidate, University of San Francisco School of Law (2013); B.A. Business Administration, 2009, University of San Diego. For her outstanding guidance and helpful comments on prior drafts, I am grateful to University of San Francisco School of Law Professor, Susan Freiwald. Her thought-provoking and challenging courses in Cyberspace Law and Information Privacy inspired this Comment. The author gratefully thanks Jackie Falk for her invaluable assistance and editing of prior drafts, and the *University of San Francisco Law Review* editors and fellow staff members for their support.

1. VIKTOR MAYER-SCHÖNBERGER, DELETE: The Virtue of Forgetting in the Digital Age 1, 110 (2009).
2. *Id.* at 1.
3. *Id.*
4. *Id.*
5. *See* Lauren Sher, *Miss Seattle Insists She Doesn't Hate Seattle After Twitter Rant*, ABC NEWS (Mar. 7, 2012), http://abcnews.go.com/blogs/headlines/2012/03/miss-seattle-insists-she-doesnt-hate-seattle-after-twitter-rant/ (relating the story of Miss Seattle's controversial Tweets and her subsequent apology); Louise Boyle, *'I Can't Stand Rainy Seattle and the Annoying People': Newly-crowned Miss Seattle Apologises After Twitter Rant*, MAIL ONLINE (Mar. 6, 2012), http://www.dailymail.co.uk/news/article-2111252/Beauty-queen-Miss-Seattle-criticises-city-Twitter.html (providing screen-shot photographs of Miss Seattle's Tweets in perfect digital form).

tered and won the Miss Seattle scholarship pageant, she tweeted that she was "seriously . . . hating Seattle right now" and wanted to be taken "back to [Arizona]!!!" because "[u]gh" she could not "stand cold rainy Seattle and the annoying people."[6] After Ahn was crowned Miss Seattle in March 2012, a Seattle reporter disclosed her tweets to the public.[7] This report inspired local and national criticism for the pageant winner on television, radio, in news articles and blog commentary.[8] Seattle radio personality, Linda Thomas, remarked that "[o]n her Twitter feed, [Miss Seattle] frequently uses the word 'annoyed,' so perhaps it's just her favorite word. [Miss Seattle] should reconsider the way [she] uses social media if she wants to be a public figure."[9] Even though Ms. Ahn later deleted her controversial tweets, they still remain in perfect permanent digital form on the Internet through copies, on blogs, and in articles discussing the incident.[10] The Internet's permanent digital memory will associate the tweets and commentary with Ms. Ahn for the rest of her life. Thus, "far from giving us a new sense of control over the face we present to the world, the Internet is shackling us to everything that we have ever said, or that anyone has said about us."[11]

For both Stacy Snyder and Miss Seattle 2012, the Internet remembered what both wanted to forget. Stories like these are becoming more common. It is becoming harder for users to separate themselves from online content that negatively affects their offline work life, personal life, school life, and, for Miss Seattle 2012, their pageant life.[12]

Many employers use individuals' online presence and history in their hiring processes. Seventy percent of United States recruiters report that they have rejected candidates because of information they found online, such as photos, discussion-board conversations, and

6. Linda Thomas, *New Miss Seattle Was 'Annoyed' With Us*, NEWS CHICK BLOG (Mar. 5, 2012, 2:47 PM), http://mynorthwest.com/646/638888/New-Miss-Seattle-was-annoyed-with-us?page=4.

7. Rene Lynch, *Miss Seattle Sorry for Using Twitter to Bash Seattle*, L.A. TIMES (Mar. 7, 2012), http://articles.latimes.com/2012/mar/07/nation/la-na-nn-miss-seattle-sorry-twitter-20120307.

8. *Id.*; *see also* Sher, *supra* note 5 (providing examples of television, radio, news, and blog media coverage of Miss Seattle's story); Boyle, *supra* note 5 (same); Thomas, *supra* note 6 (same).

9. Thomas, *supra* note 6.

10. *See, e.g.*, *id.*

11. Jeffery Rosen, *The Web Means the End of Forgetting*, N.Y. TIMES (July 21, 2010), http://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html?pagewanted=all [hereinafter Rosen, *The End of Forgetting*].

12. *Id.*; Thomas, *supra* note 6.

participation or membership in controversial groups.[13] Some employers even demand employees and applicants give them their social networking names and passwords.[14] College coaches have also been known to require the same from their athletes.[15]

When perfect memory is the norm, it poses the risk of great social and economic harm. The Internet's perfect digital memory, automatic archives, and worldwide audience harmed Stacy Snyder, Miss Seattle 2012, and countless unknown others' online and offline reputations.[16] These examples illustrate that people who post content to the Internet assume the risks, foreseeable and unforeseeable, associated with what they publish. Individuals now assume the risk that what they do on the Internet, especially in social media forums, is accessible to the entire world.[17] This leaves users with two choices: either choose to be selective in his or her online interactions, or choose not to and accept the consequences that result from unfiltered actions.

13. Rosen, *The End of Forgetting*, *supra* note 11.

14. Tierney McAfee, *Colleges, Employers, Demand Access to Applicants' Facebook Accounts*, NBC WASH. (Mar. 6, 2012), http://www.nbcwashington.com/news/tech/Colleges-Employers-Demand-Applicants-Facebook-Passwords-141572703.html. In California and Maryland, state laws prohibit employers from requesting or demanding access to the social network profiles of employees or potential applicants. *See* CAL. LAB. CODE § 980 (West 2013) (signed into law on Sept. 27, 2012); MD. CODE ANN. LAB. & EMPL. § 3-712 (LexisNexis Supp. 2012) (Maryland's law became effective Oct. 1, 2012). In these states, employers also cannot require employees or job applicants to give them social network user names and passwords. CAL. LAB. CODE § 980; MD. CODE ANN. LAB. & EMPL. § 3-712. Congress has proposed offering similar protection through a proposed federal bill. *See* Password Protection Act of 2012, H.R. 5684, 112th Cong. (2012), *available at* http://www.govtrack.us/congress/bills/112/hr5684/text.

15. Some college coaches or administrators require college athletes to "friend" them and allow viewing access to the college athletes' private posts. McAfee, *supra* note 14. California Governor Jerry Brown signed S.B. 1349 into law on September 27, 2012, prohibiting public and private post-secondary educational institutions from demanding social media passwords and viewing access to social media profiles of California students, prospective students, or students groups. S.B. 1349, 2011-2012 Reg. Sess. (Cal. 2012), *available at* http://leginfo.legislature.ca.gov/faces/billTextClient.xhtml;jsessionid=cd4ee55e9a736436443b9249afea?bill_id=201120120SB1349.

16. A Google search of Miss Seattle 2012's name, Jean-Sun Hannah Ahn, turns up links to articles criticizing her controversial tweets about Seattle. Jean-Sun Hannah Ahn Google Search, GOOGLE, http://www.google.com/ (type "Jean-Sun Hannah Ahn" in the search field; click "enter").

17. *See Terms of Service*, TWITTER, https://twitter.com/tos (last visited Apr. 7, 2013) ("What you say on Twitter may be viewed all around the world instantly. You are what you Tweet!"); Erik Lacitis, *Miss Seattle's Missteps on Twitter Provide a Lesson in Social Media 101*, SEATTLE TIMES (Mar. 9, 2012), http://seattletimes.com/html/localnews/2017713035_twitter10m.html ("There is no such thing as a private tweet. . . . If what you tweeted would run as a headline, would you be OK with that? If not, don't use it." (internal quotations omitted)).

This Comment will: (1) call attention to the type and amount of harm a permanent digital record on the Internet can cause to a person's reputation; (2) argue for meaningful and effective user control over personal information on the Internet; (3) recommend recognition of a "delete-by-default" approach to information stored about users and the content they generate; and (4) propose legislation that gives users more control over the data they create on the Internet. This Comment argues that Congress should enact a law requiring websites that allow users to create content to provide data expiration settings that would automatically delete original user-posted content at a user-selected time. Under this proposed law, users will have more control over their information posted online that is stored on website servers. The proposal combines regulation and technology to increase user control over self-created data. This Comment argues further that "permanency-by-default" does not have to be the controlling norm on the Internet when "[a]n entire generation . . . [grows] up in a very different world, one where people will accumulate detailed records beginning with childhood that will stay with them for life wherever they go."[18]

I. The Current Problem: Permanent Digital Memory

A. Reputational Harm to Users as a Result of Permanent Digital Memory

The "openness" of the Internet as well as digital advances, cheap storage, and improved accessibility have caused permanent *electronic remembering* to be the new social norm and *electronic forgetting* to be the exception.[19] Through digital technology, an exact replica of information can be transferred to others at virtually no cost with a simple click of a mouse.[20] This ease, coupled with permanently available information, creates a serious risk of harm to one's reputation, stifles one's online interaction and communication, and limits one's ability to control his or her own image.[21] "Today, forgetting has become costly and

18. DANIEL J. SOLOVE, THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET 11 (2007).

19. *See* Mayer-Schönberger, *supra* note 1, at 52, 101–06.

20. *See generally* Boyle, *supra* note 5 (providing a screen-shot copy of Miss Seattle's original Tweets from her Twitter account page).

21. *See* Felix Gillette, *Snapchat and the Erasable Future of Social Media*, BLOOMBERG BUSINESSWEEK (Feb. 07, 2013), http://www.businessweek.com/articles/2013-02-07/snapchat-and-the-erasable-future-of-social-media (describing the risks associated with the Internet's permanent record and its affect on user behavior); Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119, 144–45 (discussing context concerns resulting from

difficult, while remembering is inexpensive and easy."[22] Currently, most ways to "forget" online require manual deletion and a significant amount of wait time for removal from the server.[23] Manual deletion, whether used to prevent or react to harm, does not sufficiently incorporate the concept of electronic forgetting as contemplated by this Comment. Even though users can instantly remove user-generated content from the direct view of other users through privacy settings and manual deletion, such removal does not address the permanency problem that this Comment aims to address for a number of reasons. First, websites require users to act after posting content, but do not provide a deletion setting that governs removal during or prior to the act of posting.[24] Second, websites provide piecemeal deletion options rather than general settings that apply to categories of content.[25] Finally, websites, which have an incentive to retain data (and in some cases, sell that data to third parties), control the removal of data.[26] This Comment aims to address these failures.

---

how easily content shared in one context and meant for a particular audience can be exposed and misunderstood by a multitude of unintended and unanticipated viewers). Concerns regarding disclosure of non-consenting third parties' information is beyond the scope of this paper. For a discussion of this issue see, for example, Lawrence Lessig, *Privacy and Attention Span*, 89 GEO. L.J. 2063, 2065–66 (2001); Thomas Claburn, *YouTube Tool Blurs Faces to Protect Privacy*, INFORMATIONWEEK (Mar. 29, 2012), http://www.informationweek.com/news/security/privacy/232700524 (describing Google-owned YouTube's face-blurring technology as a response to privacy concerns of individuals who are depicted in another user's posted video without their consent).

22. MAYER-SCHÖNBERGER, *supra* note 1, at 92.

23. *See, e.g.*, Jacqui Cheng, *Three Years Later, Deleting Your Photos on Facebook Now Actually Works*, ARS TECHNICA (Aug. 16, 2012, 7:05 AM), http://arstechnica.com/business/2012/08/facebook-finally-changes-photo-deletion-policy-after-3-years-of-reporting/ (describing how in 2009 it could take one to three years to have photos removed from Facebook's server, while now it takes around thirty days).

24. *See Deleting a Tweet*, TWITTER (last visited Apr. 7, 2013), https://support.twitter.com/articles/18906-how-to-delete-a-tweet [hereinafter *Deleting a Tweet*].

25. *See, e.g.*, *id.* ("We do not provide a way to bulk-delete Tweets. You can only delete Tweets manually, one by one."); *see also* Mustaza Mustafa, *How to Delete All Facebook Messages in One Click [Quicktip]*, HONGKIAT.COM (last visited Apr. 7, 2013), http://www.hongkiat.com/blog/mass-delete-facebook-messages/ (describing Facebook's multiple click delete options and a Google Chrome extension that provides a one-click delete option for Facebook users).

26. *See* Gillette, *supra* note 21 (describing the present business model of social media websites—acquiring as much user data as possible to sell to marketers); *Privacy Policy*, SNAPCHAT, http://www.snapchat.com/privacy (Feb. 20, 2013) (notifying users how and what information is collected and explaining the website's policy for deleting user data). *See generally Data Use Policy*, FACEBOOK (Dec. 11, 2013), https://www.facebook.com/about/privacy/other (describing how user data is used and shared); James Vincent, *Facebook Wants Your Data, and Magic Legalese Won't Keep It Away*, NEWSTATESMAN.COM, (Nov. 28, 2012, 4:28 PM), http://www.newstatesman.com/technology/2012/11/facebook-wants-your-data-and-

A person's reputation has high social, personal, and economic value, and is essential for social interaction.[27] The United States Supreme Court has held that "[s]ociety has a pervasive and strong interest in preventing and redressing attacks upon reputation."[28] The scholar Robert Post views reputation as a form of property and argues that legal recognition of a dignity interest is necessary to protect the time and effort a person invests in earning, developing, and preserving his or her reputation.[29]

Online reputation management companies offer assistance designed to maintain digital reputations, however, as this Comment will discuss, these reputation companies are insufficient to deal with the problem of permanent digital memory. For a fee, the California-based company Reputation.com monitors its client's online reputations, contacts individual websites to request the take down of offending content, and uses technology to "bombard the Web with positive or neutral information about its customers" to ensure positive information shows up first on a Google search.[30] Although Internet users may control the content they generate by manually deleting it, selectively and strategically censoring what they say, and using online reputation management companies, these strategies do not provide users with sufficient control. In today's world where a person's "online resume" or "Google CV" is just as important as his or her offline reputation,[31] Congress needs to recognize a dignity interest in online reputation and provide users' greater control over their content.

magic-legalese-wont-keep-it-away (explaining Facebook's policy changes, which allow for greater retention and broader use of user data and personal information).

27. *See generally,* SOLOVE, *supra* note 18, at 30–35 (describing the value of reputation and how reputation affects social and economic interactions).

28. Rosenblatt v. Baer, 383 U.S. 75, 86 (1966); SOLOVE, *supra* note 18, at 34 (describing the value of reputation).

29. Robert C. Post, *The Social Foundation of Defamation Law: Reputation and the Constitution*, 74 CAL. L. REV. 691, 694, 707-08 (1986); *see also* SOLOVE, *supra* note 18, at 34.

30. Rosen, *supra* note 11 at 35; *see also* Danielle Cahill, *Why Online Reputations Matter*, HERALD SUN (Jan. 18, 2011), http://www.heraldsun.com.au/ipad/why-online-reputations-matter/story-fn6bfkm6-1225989811452 (discussing how Reputation.com offers clients such as families, corporations, and individuals tailored services starting at $14 to monitor and protect both reputations and privacy on the web); REPUTATION.COM, http://www.reputation.com/ (last visited Apr. 7, 2013).

31. *Part I: Answers to Questions About Internet Privacy*, N.Y. TIMES (July 26, 2010), http://bits.blogs.nytimes.com/2010/07/26/part-i-answers-to-questions-about-internet-privacy/?ref=magazine (detailing the responses of Michael Fertik, founder of ReputationDefender, and Paul Ohm, law Professor at the University of Colorado, to reader questions about online reputation, use of social media, and maintaining privacy on the Internet).

B. Benefits and Costs of Perfect Digital Memory

There are both benefits and costs to a permanent digital record. The costs, however, outweigh the benefits. Benefits of perfect digital memory include increased accuracy of information; improved efficiency in online market transactions; preservation of a historical record; increased access to information and knowledge; and increased trust in interactions and market dealings with others.[32] Social media profiles can also have a positive effect when it comes to hiring prospective employees as profiles provide insight into applicants' personalities, interests, skills, and interactions with others.[33] Perfect digital memory permits more rapid and wider dissemination of information, which in turn enables economic growth and increases accountability on the Internet.[34] The proposed legislation does not eliminate these benefits. On the contrary the proposed legislation only minimally restricts accountability because users would be able to permanently delete their self-generated content, but would not be able to remove the user's replicated content that third parties copy or generate. It insignificantly affects preservation of a historical record because media and news sources would still be able to report on and record user content and furthermore, the majority of user-generated content is not likely to have historical value. The proposed legislation does not affect the dissemination of information because third parties would still be able to copy and redistribute user-generated information. Employers would still be able to view and access potential employee profiles although with the proposed legislation an employee would possess more control over the information an employer could access. The proposed legislation minimally affects the level of trust in market dealings with others because other users will still have access to informa-

32. MAYER-SCHÖNBERGER, *supra* note 1, at 93–94.

33. In a recent CareerBuilder Survey of hiring managers on the benefits social media provides employers and applicants during the hiring process, "58% of the respondents said that it gave them a good feel for the candidates personality, 55% said the profiles conveyed a professional image, and 54% said that information they found supported the candidate's professional qualifications. 51% said that the social media profiles displayed a well-rounded candidate, showing a wide range of interests, 49% cited great communication skills, 44% said [social media public profiles] displayed the candidate's creativity, while 34% said that other people's online recommendations made a difference." Nancy Messieh, *Survey: 37% of Employers Look Up Employees on Social Media*, THE NEXT WEB, SOCIAL MEDIA BLOG (Apr. 18, 2012), http://thenextweb.com/socialmedia/2012/04/18/survey-37-of-your-prospective-employers-are-looking-you-up-on-facebook/.

34. Rosen, *The End of Forgetting*, *supra* note 11; *see also* Globalization 101, INFO. TECH. BLOG, *available at* http://www.globalization101.org/information-technology/ (last visited Apr. 5, 2013) (discussing how information technology and increased dissemination of information foster economic growth).

tion about the user that third parties can provide. Social media users are also aware that not all users can be trusted, and it is likely that if a user is not trustworthy the market will make this known.[35]

Permanent digital records have several defects that outweigh the potential benefits. First among these is the high user-costs associated with such digital records. Permanent digital records make it more difficult for people to avoid their pasts on the Internet. "[A permanent] record will affect our ability to define our identities, to obtain jobs, to participate in public life, and more,"[36] because a user may not be able to escape past actions. The Internet automatically and permanently associates an individual's past actions with him or her; however, such past actions may no longer accurately reflect the individual's identity.[37]

Perfect digital memory can also make self-exploration and self-expression more costly. In 2002, a fifteen-year-old boy named Ghyslain filmed himself enthusiastically pretend-fighting an invisible opponent with a lightsaber-like object, sound effects included.[38] Although Ghyslain did not intend for others to see the video, kids at his school discovered the video and uploaded it to the Internet, and the "Star Wars Kid" became an instant hit.[39] Ghyslain's two minutes of youthful self-expression resulted in numerous websites providing edited versions of the video where users added insulting comments. Popular television series like Family Guy and Arrested Development also made fun of Ghyslain.[40] Major print and online newspapers and magazines wrote about Ghyslain's story and fueled worldwide interest in the video.[41] Remarkably, fans of the "Star Wars Kid" signed an unsolicited online petition lobbying George Lucas' film company to give Ghyslain a role

35. *See, e.g.*, Helen Popkin, *Facebook: More Than 83 Million Users Are Fake*, NBC NEWS (Aug. 3, 2012), http://www.nbcnews.com/technology/technolog/facebook-more-83-million-users-are-fake-919873 (reporting that 8.7% of Facebook's active monthly users have fake accounts).

36. SOLOVE, *supra* note 18, at 17.

37. Samuel Axon, *The "Star Wars Kid": Where Is He Now?*, MASHABLE ENT. (Jun. 3, 2010), http://mashable.com/2010/06/03/star-wars-kid/ (describing how a playful childhood video continues to follow the now-grown-up Canadian lawyer).

38. *Id.*

39. *Id.*

40. *Id.*

41. Amy Harmon, *Compressed Data: Fame Is No Laughing Matter for the 'Star Wars Kid'*, N.Y. TIMES (May 19, 2003), http://www.nytimes.com/2003/05/19/business/compressed-data-fame-is-no-laughing-matter-for-the-star-wars-kid.html; *see also* Jaime Holguin, *The Strange World of Web Celebs*, CBS NEWS (Feb. 11, 2009), http://www.cbsnews.com/8301-18563_162-584216.html; *Star Wars Kid Is Top Viral Video*, BBC NEWS, (Nov. 27, 2006), http://news.bbc.co.uk/2/hi/entertainment/6187554.stm.

in the film Star Wars Episode III, and although unsuccessful, the petition garnered over 145,000 signatures.[42] After the incident, Ghyslain dropped out of high school, suffered from depression, and sought psychiatric care.[43] Even today he cannot separate his identity from the video.[44]

The legislation this Comment proposes[45] could not have redressed the harm suffered by Ghyslain under the particular circumstances of his case, since a third party posted the video to the Internet and others then copied it. However, if the legislation that this Comment proposes were in place when Ghyslain uploaded the video to his own Facebook account, Ghyslain could have set the video to delete after a short amount of time, before a third party was able to copy his content.

Ghyslain's story illustrates that the more information appears in permanent digital form and is accessible to anyone, anywhere, the harder it will be to avoid ties to personal information by physically moving to another social circle, school, job, or state.[46] A person's online identity effectively travels with that person forever once the data is posted online.[47] Daniel Solove aptly notes that, "[t]he Internet is bringing back the scarlet letter in digital form – an indelible record of people's past misdeeds."[48] Digital memory persists forever. Besides being difficult and costly, it creates the risk that a picture or comment posted while a person is young may hinder his or her admission to college or employment attractiveness.[49] Self-censorship, harm to repu-

42. *Ghyslain Petition to Lucasfilm Ltd.*, PETITIONONLINE, http://www.petitiononline.com/Ghyslain/petition.html (last visited Apr. 5, 2013).

43. *Star Wars Kid Files Lawsuit*, WIRED (July 24, 2003), http://www.wired.com/culture/lifestyle/news/2003/07/59757 [hereinafter *Star Wars Kid*]; Alex Pasternak, *After Lawsuits and Therapy, Star Wars Kid is Back*, MOTHERBOARD, http://motherboard.vice.com/blog/after-lawsuits-and-therapy-star-wars-kid-is-back (last visited Apr. 5, 2013).

44. *See* Axon, *supra* note 37 (describing how the video continues to impact Ghyslain's life).

45. *See infra* Part II.

46. *See Star Wars Kid*, *supra* note 43 (describing Ghyslain's current work as a law student and President of a non-profit while noting that the video still followed him).

47. *See* Mayer-Schönberger, *supra* note 1, at 52.

48. SOLOVE, *supra* note 18, at 11.

49. In a 2011 Kaplan Test Prep survey of college admissions counselors', 24% of respondents admitted to going onto applicants' public Facebook or other social networking page, and 12% admitted that online discovery of something about an applicant negatively affected an applicant's application. KAPLAN, HIGHLIGHTS FROM KAPLAN TEST PREP'S 2011 COLLEGE ADMISSIONS OFFICERS SURVEY (2011), *available at* http://press.kaptest.com/wp-content/uploads/2011/09/Kaplan-Test-Preps-2011-Survey-of-College-Admissions-Officers.pdf; A recent CareerBuilder Survey, which questioned approximately 2,300 hiring managers and human resources professionals in February and March 2012, indicated that at least

tation, and persistent criticism of youthful indiscretions of those who have matured beyond them are also costs of perfect digital memory. These high costs to users outweigh the minimal effect that the legislation this Comment proposes has on the above benefits, and justify the legislation. The proposed legislation, which requires social media websites to allow user-generated information to be electronically forgotten through user-selected delete settings and only minimally restricts user accountability,[50] is necessary to alleviate the harms discussed above.

C. Scholars' Proposed Solutions to Address the Costs of Perfect Digital Memory

Legal scholars have suggested a variety of ways to address reputational harm from the Internet's permanent record keeping. One such scholar, Jonathan Zittrain, argues that people should be allowed to declare a form of "reputation bankruptcy," similar to personal financial bankruptcy, which would allow them to erase various categories of sensitive information.[51] Such sensitive information may relate to personal or professional mistakes that are widely publicized, indiscretions such as drunk driving and drug charges, and personal, dating, and professional matters that influence a person's reputation.[52] Under Zittrain's view, it might not be feasible for individuals to selectively delete entire records of sensitive information about them without a cost.[53] Therefore, Zittrain posits that both good and bad information would disappear together to serve "[a]s a safety valve against excess[ive] experimentation."[54] Zittrain suggests that we should implement the idea of electronic forgetting into the digital world and notes that this *digital do over* approach would work best with social networking sites where people interact with one another by sharing information in the same network.[55] Under this approach, Zittrain emphasizes that individuals should be able to "express a choice to deemphasize if not entirely

37% of employers look to the public social media profiles of prospective employees before making a final decision. The study indicated that one third of hiring managers said that negative content on such profiles led to applicants not getting a position: 49% cited inappropriate photographs; 45% cited discussion about drinking and drug use; 35% cited speaking poorly of a previous employer; 28% cited discriminatory remarks; and 22% cited lying about qualifications. Messieh, *supra* note 33.

50. *See infra* Part II.A.

51. JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET AND HOW TO STOP IT 228–31 (2008).

52. *Id.*

53. *Id.* at 229.

54. *Id.*

55. *Id.* at 228–29.

delete older information that has been generated about them by and through various systems: political preferences, activities, youthful likes and dislikes."[56]

Zittrain's view of reputation bankruptcy, while providing users with more control over their reputations, asks too much from the user because it requires the user to: (1) formally declare reputation bankruptcy, which may carry a stigma; (2) "forget" after he or she suffers harm; and (3) forgo association with positive information in exchange for disassociation from unwanted information.[57] It also does not require any independent action from the social network website.[58] Independent website action is crucial because in order to successfully implement a norm of forgetting on the Internet action from both websites and users is necessary. When websites are required to act to implement a specific service, like deletion options, the power gap that exists between websites and users is narrowed because both are acting to implement the norm; it is no longer a one-sided effort on the part of the weaker party—the user.

In a recent *New York Times Magazine* article, Jeffery Rosen described another solution set forth by Paul Ohm. Ohm's solution aims to address harms in the employment relationship by implementing a discrimination ban for specific online content.[59] Ohm suggests that employers should not be allowed to fire or refuse to hire anyone on the basis of legal off-duty conduct that is revealed in public profiles on Facebook or Google profiles.[60] Ohm supports the passage of "a prohibition on the sorts of information employers can and can't consider when they hire someone."[61] Many states already have laws that prohibit employers from discriminating against employees for legal, non-employment related conduct like smoking.[62] State legislators could extend such laws to shield certain categories of information about a person, like distasteful Facebook pictures, offensive status updates, or other legal but controversial information from the employer's hiring decision.[63] While Ohm's solution is tenable, it is insufficient for several reasons. First, it fails to address the permanency problem. Sec-

56. *Id.* at 229.

57. ZITTRAIN, *supra* note 51, at 229.

58. *Id.*

59. Rosen, *The End of Forgetting*, *supra* note 11.

60. *Id.*

61. *Id.*

62. *Id.* (listing California, New York, Colorado, and North Dakota as states with such laws).

63. *Id.*

ond, it requires no change from social network websites. Lastly, it offers users protection from, not control over, their reputations.

Viktor Mayer-Schönberger presents arguably the best solution, proposing that digital storage devices, such as computers and mobile phones, should automatically delete information that reaches a user-set "expiration date."[64] For example, when a user saves a document, in addition to naming the document and selecting a location to store it on the hard drive, the user would also select an expiration date.[65] Mayer-Schönberger argues that the Internet must develop the ability to mimic human forgetting through user-applied, built-in expiration dates to each piece of data.[66] Through the idea of expiration functions, Mayer-Schönberger emphasizes that the concept of forgetting can and should be reintroduced into our daily activities and routines on the Internet.[67] Mayer-Schönberger recognizes that there is a "lifespan of information" that people choose to make available on the Internet.[68] Expiration dates, he argues, are "designed to confront us with (and thus remind us of) the 'finiteness of information'—in other words, that information is inexorably linked to a point (or period) in time, and that over time most information loses its informational value."[69] Mayer-Schönberger's solution, however, does not go far enough because it does not require social network websites to provide users with an expiration date mechanism. This Comment proposes legislation that requires websites to provide such a mechanism.

II. The Online User Data Expiration Act

A. Statutory Provisions of the Online User Data Expiration Act

Mayer-Schönberger's idea of expiration settings for data on the Internet by mandating that specific websites offer users deletion technology that provides control over the data they generate is included in the proposed legislation. The proposed legislation, the Online User Data Expiration Act ("OUDEA"), specifically requires all U.S. websites that allow users to post self-generated content to provide, as a free

64. MAYER-SCHÖNBERGER, *supra* note 1, at 171-73.

65. *Id.* at 171.

66. Rosen, *The End of Forgetting*, *supra* note 11.

67. MAYER-SCHÖNBERGER, *supra* note 1, at 172-73.

68. *Id.* at 173.

69. *Id.* at 171.

service, data destruction technology for all such original, user-generated content. The provisions of OUDEA[70] would be as follows:

§ 1: Definitions.

a. "Agency" refers to the Federal Trade Commission ("FTC") or another administrative entity to be formed and funded by Congress to enforce these provisions.

b. "Communicative Act" refers to the method of Notice utilized by the Website. It must inform the User that his or her Content has been removed and deleted. The Act must be in the form of email, pop-up window, notification system, weekly and/or monthly report, or other similar notification system and must identify and summarize the deleted Content and action(s).

c. "Content" refers to any: text; word; photo; comment; "like"; "tweet"; video; review; music; graphic; and/or any combination of the above. "Content" also includes any other communicative or expressive act having a similar effect as those listed above.

d. "Data Expiration Setting" refers to a control option that each Website in § 2 (a) must provide in its Website Service. The Data Expiration Setting must allow Users to manually choose between preset time ranges of various durations. The Data Expiration Setting must offer the use of Expiration Technology approved by the Agency that has the capability of destroying data.

e. "Expiration Technology" refers to technology approved by the Agency that is capable of independently and permanently deleting original data.

f. "Independent Panel" or "Panel" refers to a review committee that will comprise of three officials. Creation of the Panel, its procedures, and selection of its officers shall be determined and funded by Congress. The FTC or other Congress-selected agency is in charge of regulating the Panel.

g. "Notice" refers to a Communicative Act from the Website to the User. It is required to inform Users of Expiration Technology and Expiration Settings, as well as any updates or changes to the Technology or Settings. Notice is required within a reasonable amount of time, but no later than two (2) weeks, after the deletion of a User's User-Generated Content.

70. The Online User Data Expiration Act ("OUDEA") is the author's original legislation, meant as a guideline for what this type of legislation should look like in order to effectively protect users' deletion rights.

h. "Service" refers to any part of a Website's offerings or function that is provided at a network address on the Internet.

i. "User" refers to any person, IP address, computer, entity, or thing that electronically communicates with, uses, accesses, or browses the Website.

j. "User-Generated" refers to the specific act of the User whereby Content is created, added, posted, edited, or placed on the Website. It includes but is not limited to Content in which the User would have a copyright interest.

k. "Website" refers to any Internet actor or entity with a .com, .org, .edu, .gov, any other generic top-level domain used on the Internet[71] or domain name that permits user access to a service—including the posting of text, information, sound, images, video, or any combination of the above—and that allows users to create, generate, or enter content onto its site, which is then made either visible or audible on the Internet actor or stored on the Internet actor's server. Private and public entities are included.

§ 2: Mandatory Provisions.

a. All Websites must provide a Data Expiration Setting and corresponding Expiration Technology as a free Service to their Users. The Data Expiration Setting must apply to original User-Generated Content. Each Website must notify its Users of the Expiration Technology and provide clear, unambiguous, and meaningful instructions on how to use the Data Expiration Setting. Such Notice must explain what happens to the User-Generated Content upon deletion.

b. A Data Expiration Setting must be provided for all original User-Generated Content and must:

1. be easy to use and not overly time consuming for the User;

2. provide meaningful expiration options, which the User can freely reset without limit and must range from, but not be limited to: one (1) minute to never expire; and

3. provide Notice.

c. Expiration Technology must be implemented within six (6) months from the passage of OUDEA. Prior to, or on the first day OUDEA becomes effective (six (6) months after passage), each Website must submit to the Agency a report in writing:

1. describing the Expiration Technology used;

71. *See generally Top-Level Domains (gTLDs)*, ICANN.ORG, http://archive.icann.org/en/tlds/ (last visited Apr. 7, 2013) (describing generic top-level domains).

2. establishing that the Expiration Technology is either Agency pre-approved or that the Expiration Technology used is equivalent in all respects to the Agency pre-approved version;

3. listing and explaining Expiration Technology options and functions; and

4. identifying Notice procedures and methods for compliance.

d. Websites shall not retain, cache, or copy any User-Generated Content past the user's specified expiration date for such Content. All traces of User-Generated Content must be removed from a website's server upon the user's-specified expiration date.

§ 3: Enforcement.

a. A violation for failure to comply with § 2 of OUDEA will result in a fine of twenty-five thousand ($25,000) U.S. dollars.[72] Full compliance with OUDEA must be met within 180 days from the date finding a violation of compliance. For every week thereafter, a three thousand ($3,000) U.S. dollar per day fine will result until full compliance is met.[73]

1. A Website may respond to violation allegations and is entitled to a hearing by Independent Panel.

2. Upon a finding by the Panel that a Website was in compliance, the twenty-five thousand ($25,000) U.S. dollar fine will not apply. If the Panel finds a Website made reasonable, good faith efforts to comply with OUDEA, but nonetheless was not in compliance, the twenty-five thousand ($25,000) U.S. dollar fine will not apply on the condition that full compliance with OUDEA be met within one hundred eighty (180) days from the date of the Panel's finding.

3. Upon a finding by the Panel of a Website's failure to delete from its server all copies of the User-Generated Content upon the User's Data Expiration Setting, that User will have a private right of action against the offending Website for special and general damages

72. I base my enforcement penalty amounts on the Digital Millennium Copyright Act ("DMCA"), where civil liability for copyright infringement ranges from an order to pay either actual damages or "statutory" damages of not less than $750 and not more than $30,000 per work infringed, assuming that the infringement was not willful. If the infringement is willful, statutory damages increase. 17 U.S.C. § 504 (2006).

73. The monetary amount of these penalties are intended to serve as a deterrence to noncompliance by large and small website companies. The amounts were reached based on the following considerations: the DMCA penalties listed above (§ 504); deterrence interests; the freedom of a business to operate, fostering business growth, encouraging website to offer services where users can create data; and fairness interests to websites of all sizes. These amounts are included only as guidelines for Congress to follow when considering implementing such legislation.

of up to thirty thousand ($30,000) U.S. dollars per finding, with additional attorneys' fees and costs provided.

4. Any person who is entitled to bring a private right of action on his or her own behalf against an allegedly violating Website for an act or practice declared unlawful by §2 of OUDEA may bring a class action against such Website(s) on behalf of any class of persons of which he or she is a member and which has been harmed by such unlawful act or practice. Recovery shall be limited to actual harm suffered by the person or persons, with additional attorneys' fees and costs provided. This paragraph is not intended to create or permit class action relief where not permitted by state law.

B. OUDEA's Model Technology

Expiration technology is a feasible option to deal with permanent digital memory, and software developers continue to create various forms of it.[74] Presently, OUDEA's ideal standard for expiration technology would be similar to the security software used by a mobile phone application that physicians use on their mobile devices called TigerText.[75] TigerText uses technology that gives users a privacy-fo-

74. *See, e.g.*, John Markoff, *New Technology to Make Digital Data Self-Destruct*, N.Y. TIMES (July 20, 2009), http://www.nytimes.com/2009/07/21/science/21crypto.html (describing the University of Washington's data deletion software called Vanish); Michael Zhang, *X-pire! Software Adds a Self-Destruct Feature to Your Digital Photos*, PETALPIXEL.COM (Jan. 17, 2011), http://www.petapixel.com/2011/01/17/x-pire-software-adds-a-self-destruct-feature-to-your-digital-photos/ (discussing the German Facebook application X-pire, which adds an expiration date to photographs that makes the photograph inaccessible and invisible at a user's preset time). Examples of applications and websites that offer forms of deletion technology include: Snapchat, Burn Note, Wickr, Facebook Poke, and TigerText.

75. At present, TigerText is the model technology for OUDEA. This section is not intended to limit OUDEA deletion technology to technology like TigerText. In the event that better, more efficient and secure technology is developed in the future, this technology should be evaluated to determine whether the interests of OUDEA are better served through the implementation of such technology. Because self-destructing data phone applications are becoming more popular, the evolution and development of lifespan-data technology is likely to improve and flourish. *See* Rheana Murray, *Facebook Poke App Can't Beat Snapchat, But Questions Raised About Security*, N.Y. DAILY NEWS, (Jan. 2, 2013), http://www.nydailynews.com/news/national/facebook-poke-app-beat-snapchat-article-1.1231380 (discussing Facebook's attempt to compete with the Snapchat app and acknowledging the need for future technology improvements); *Company Overview of TigerText, Inc.*, BLOOMBERG BUSINESSWEEK, http://investing.businessweek.com/research/stocks/private/snapshot.asp?privcapId=113895949 (last visited Apr. 6, 2013). According to TigerText.com, "TigerText offers a fully encrypted, SaaS platform for secure text messaging." *Benefits*, TIGERTEXT, http://www.tigertext.com/benefits/ (last visited Apr. 7, 2013). When a user sends a TigerText, he or she can pre-set the lifespan of the message. The message stays encrypted in transit and, upon receipt, it cannot be forwarded, stored, or copied anywhere. Once it expires, it is deleted from all servers, and from both the senders' and recipients' phones.

cused service.[76] A sender is notified through a specific set of small corresponding icons once his or her message is received, opened, and expires.[77] By using TigerText, senders can pre-set text messages to expire from one minute to thirty days after sending.[78] Upon expiration, the text will disappear from all servers and from the sender and recipient phones.[79] TigerText offers a delete-on-read setting which, once a message is opened by its recipient, counts down from fifty-nine seconds before it automatically disappears.[80] There is even a delete-history setting that erases the record of expired messages.[81] Ideally, websites should implement TigerText-like technology and use it the same way for user-generated content posted to the Internet. TigerText offers tailored features such as messaging from PCs and Macs and can easily be integrated into other networks and operating systems.[82] The level of control that TigerText provides for its users through its software design and deletion settings is the type of user control over user-generated content that OUDEA secures for users.[83]

C. How OUDEA Would Address Concerns About Permanent Digital Memory

OUDEA's provisions would enhance user control by permitting users to dictate the lifespan of the content they generate on the In-

For a more detailed description of how TigerText software works see *Frequently Asked Questions*, TIGERTEXT, http://downloads.tigertext.com/faq#11 (last visited Apr. 7, 2013) [hereinafter *TigerText FAQ*].

76. *See* Rosen, *The End of Forgetting*, *supra* note 11; TIGERTEXT, http://www.tigertext.com/ (last visited Apr. 6, 2013); Jessica Galliart, *Does It Work?: Tiger Text's Disappearing Text Messages*, EVERYTHINGICAFE.COM (Mar. 4, 2010), http://www.everythingicafe.com/does-it-work-tiger-texts-disappearing-text-messages/2010/03/04/ (explaining how TigerText works); TigerTextMedia, *TigerText Product Walkthrough for iOS*, YOUTUBE (June 15, 2011), http://www.youtube.com/watch?v=A4Z0b5gVyOQ (illustrating how to use the application and how the technology works).

77. *TigerText FAQ*, *supra* note 75. "When a message is received, the sender will see an orange box with a check. When a message is opened by the recipient, the sender will see a green circle with a check. When the message expires, the sender and recipient will see tiger paws walking across the screen." *Id.*

78. Rosen, *The End of Forgetting*, *supra* note 11.

79. *TigerText FAQ*, *supra* note 75.

80. *Id.*

81. *Id.*

82. *See For Consumers*, TIGERTEXT, http://www.tigertext.com/consumer/ (last visited Apr. 6, 2013) [hereinafter *TigerText For Consumers*] (listing TigerText features and product offerings); *Features*, TIGERTEXT, http://www.tigertext.com/features/ (last visited Apr. 6, 2013) (explaining that TigerText integrates easily with information systems).

83. "With TigerText, you, your friends and family can now say what you want, when you want—while still keeping control over your texts." *See TigerText For Consumers*, *supra* note 82.

ternet. OUDEA would allow users to direct websites to no longer hold on to their user-generated content forever,[84] while OUDEA's fines and private right of action would serve as strong enforcement mechanisms to support users' demands for the removal of user-generated content.[85]

OUDEA would make it easier for users to erase past indiscretions, photos, and comments from the Internet. OUDEA allows users to choose whether data should expire, and if so selected, the amount of time before expiration occurs.[86] Under OUDEA, a Facebook user could set her status updates to "expire" after seven days, or a Twitter user, like Miss Seattle 2012, could set her tweets to expire after fourteen days.[87] Users' sense of protection from future, unknown harms caused by their user-generated content would improve and self-censorship would lessen because there would be fewer ways for one's past online interactions to come back to haunt them. Although OUDEA would not protect users from another person who copies, reposts, or saves their content, it would require that every trace of their original content be deleted from Facebook and Twitter sites and their servers, which would reduce the availability of such content.[88]

D. OUDEA Would Help Achieve a Delete-by-Default Norm

OUDEA embodies a major step forward towards a delete-by-default approach for user-generated information. Even though OUDEA would require websites to provide deletion technology for user-generated content and to abide by user choice,[89] users would have to take advantage of this expiration technology to make delete-by-default the norm.

User desire for delete-by-default exists.[90] While people are clearly willing to share a tremendous amount of personal information online, they still care whether a website keeps a permanent record of their

84. *See supra* Part II.A.
85. *See supra* Part II.A.
86. *See supra* Part II.A.
87. *See supra* Part II.A.
88. *See supra* Part II.A.
89. *See supra* Part II.A.
90. *See* Gillette, *supra* note 21 (describing user popularity of the Snapchat application, an app that allows users to share impermanent media with others, and user popularity of former start-up Drop.io's data expiration settings); Greg Crowe, *Self-Deleting E-mails: An Enterprise Nightmare?*, GCN BLOG (Jan. 29, 2013, 4:58 AM), http://gcn.com/blogs/mobile/2013/01/self-deleting-emails-personal-protection-or-enterprise-nightmare.aspx (discussing self-destructing emails and user demand for data destruction).

personal information and online activity.[91] In a recent University of California Berkeley study, a significant majority of Americans, ranging from ages eighteen to sixty-five and over, agreed that laws should require websites to delete all stored information about them.[92] Because these individuals support the passage of a law that would require websites to delete stored personal information, they would likely support legislation like OUDEA which requires websites to delete their user-generated content.[93]

E. OUDEA Respects Speech Interests Which Europe's Proposal Fails to Do

European and American laws conflict in their treatment of privacy and free speech interests in the context of a right to be forgotten. European law is much more protective of privacy rights and less protective of free speech than United States law, which is more protective of speech interests and censorship concerns and less protective of privacy.[94]

In response to increased awareness of privacy concerns regarding personal information on the Internet, the European Union has recently proposed an expansive and highly protective privacy right known as the "right to be forgotten."[95] The new data protection proposal provides European Union citizens the right to request that their data be deleted by third-party providers, including social networks like Facebook, Google+, and Twitter, if no legitimate reason to keep the

91. Gillette, *supra* note 21; *see also* Jason Gilbert, *Burn Note: Email Messages That Self-Destruct Automatically After One Minute*, HUFFINGTON POST (Jan. 31, 2012), http://www.huffingtonpost.com/2012/01/31/burn-note-email-messages-self-destruct_n_1245480.html (explaining how Burn Note works and its benefits to potential customers).

92. In response to the question, "Do you think there should be a law that requires websites and advertising companies to delete all stored information about an individual, or do you feel such a law is not necessary?," 92% of 975 respondents answered, "[y]es [there] should be a law" (yes responses by age group were as follows: 88% ages 18–24; 91% ages 25–34; 90% ages 35–44; 94% ages 45–54; 94% ages 55–64; and 90% ages 65+). CHRIS HOOFNAGLE ET AL., HOW DIFFERENT ARE YOUNG ADULTS FROM OLDER ADULTS WHEN IT COMES TO INFORMATION PRIVACY ATTITUDES & POLICIES? 11 (2010), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1589864.

93. *See* Gillette, *supra* note 21 (describing user desire for government intervention regarding permanent social records).

94. *See* M. Patrick Yingling, *Europe: Privacy and Free Speech*, JURIST (May 25, 2010), http://jurist.org/dateline/2010/05/germany-international-concepts-of-privacy.php (describing differing American and European notions of the legal principles surrounding privacy and free speech).

95. Jeffery Rosen, *The Right to Be Forgotten*, 64 STAN. L. REV. ONLINE 88 (Feb. 13, 2012), http://www.stanfordlawreview.org/online/privacy-paradox/right-to-be-forgotten [hereinafter Rosen, *The Right to Be Forgotten*].

information exists.[96] The new right would apply to information directly published by an individual and "any information relating to a data subject."[97] The data regulation would also exempt data posted "for journalistic purposes or for the purposes of artistic or literary expression."[98] Once a user contacts Facebook with a take down request regarding specific content originally posted by the user, Facebook "must take 'all reasonable steps' on its own to identify any relevant third parties and secure the takedown of the content."[99] This requirement illustrates how European law holds Internet service providers to a duty to filter and protect the privacy of others, even when that means removing third party posts.[100] The European regulation would provide for a sanction of one million euros or up to two percent of Facebook's annual worldwide income if Facebook intentionally or negligently failed to comply with the European regulation's "right to be forgotten" provisions.[101]

In 2011, while on business in Switzerland, Peter Fleischer, Google's global privacy counsel, took to his blog to express his opinion about the right to be electronically forgotten.[102] To explain his opinion, Fleischer discusses three questions about how far the right to

96. Zack Whittaker, *European 'Right-to-Delete' Law: How Enforceable is Facebook?*, ZDNET (Nov. 14, 2011, 3:42 PM), http://www.zdnet.com/blog/london/european-8216right-to-delete-law-how-enforceable-is-facebook/909; *see also Commission Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data (General Data Protection Regulation),* at 47-50, COM (2012) 11 final (Jan. 25, 2012) [hereinafter *Proposed Data Protection Regulation*], *available at* http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf (detailing fundamental rights that justify personal information privacy protection).

97. *Proposed Data Protection Regulation*, *supra* note 96, at 41; *see also* Rosen, *The Right to Be Forgotten*, *supra* note 95, at 89.

98. *Proposed Data Protection Regulation*, *supra* note 96, at 94; *see also* Rosen, *The Right to Be Forgotten*, *supra* note 95, at 90.

99. Rosen, *The Right to Be Forgotten*, *supra* note 95, at 90 (quoting *Proposed Data Protection Regulation*, *supra* note 96, at 51).

100. "Article 17 provides the data subject's right to be forgotten and to erasure. It further elaborates and specifies the right of erasure provided for in Article 12(b) of Directive 95/46/EC and provides the conditions of the right to be forgotten, including the obligation of the controller which has made the personal data public to inform third parties on the data subject's request to erase any links to, or copy or replication of that personal data. It also integrates the right to have the processing restricted in certain cases, avoiding the ambiguous terminology 'blocking.'" *Proposed Data Protection Regulation*, *supra* note 96, at 9, 51–53.

101. *Proposed Data Protection Regulation*, *supra* note 96, at 92–94; *see also* Rosen, *The Right to Be Forgotten*, *supra* note 95, at 90–91.

102. Peter Fleischer, *Foggy Thinking About the Right to Oblivion*, PETER FLEISCHER: PRIVACY . . . ? BLOG (Mar. 9, 2011, 8:59 PM), http://peterfleischer.blogspot.com/2011/03/foggy-thinking-about-right-to-oblivion.html.

be electronically forgotten should extend including: (1) "If I post something online, should I have the right to delete it again?"; (2) "If I post something, and someone else copies it and re-posts it on their own site, do I have the right to delete it?"; and (3) "If someone else posts something about me, should I have a right to delete it?"[103] The European regulation would answer "yes" to each of Fleischer's questions.[104] However, my OUDEA proposal would answer "yes" only to Fleischer's first question; if a user posts something online he or she has a right to delete it.[105] Even though the user's right to be forgotten would not apply to user-generated content that is subsequently copied and reposted by another user, OUDEA's provisions would still increase a user's control over the information she has posted. The less content available for others to copy and repost, the lower the risk of harm. Thus, OUDEA would increase user control over personal information on the Internet, but would be narrower than the European regulation.

III. Addressing Criticisms to OUDEA

A. Users Already Have Delete Options

Some view OUDEA as unnecessary because websites already provide users with delete options.[106] Although websites and social networks allow users to delete the content they post to the Internet, this does not obviate legislation like OUDEA. At present, most websites require users to manually delete, piece by piece, the content they no longer want to remain on their sites.[107] The time and effort that requires likely deters many users from engaging in the content removal process. Because websites generally want to keep as much data about their users as possible,[108] it is no surprise that many websites do not offer deletion in bulk.[109]

103. *Id.*

104. *See generally Proposed Data Protection Regulation*, *supra* note 96; Fleischer, *supra* note 102.

105. Fleischer, *supra* note 102.

106. *Deleting a Tweet*, *supra* note 24; *see also How Do I Hide and Delete Posts from My Facebook Page? What's the Difference?*, FACEBOOK, http://www.facebook.com/help/252986458110193 (last visited Apr. 6, 2013).

107. *See Deleting a Tweet*, *supra* note 24.

108. *See* Gillette, *supra* note 21 (explaining Facebook's business model of storing and collecting user data to sell to markers and specifically noting that in January 2013, "Facebook began rolling out Graph Search, a tool to retrieve details from the pasts of its billion users").

109. According to Twitter, to delete a single tweet a user must follow these steps: (1) log in to twitter.com; (2) visit the user's profile page; (3) locate the tweet to be deleted;

Websites' default privacy practices allow users to manually alter view settings and manage their privacy settings.[110] This manual management takes time and requires users to understand what each setting does and the specific activities the settings manage. Users may simply choose to do nothing and leave their settings on the website's predetermined defaults, which usually reflect a "broadcast" approach.[111] Some are likely to argue that a website's offering of a data deletion expiration setting under OUDEA would also be associated with high user-costs,[112] especially because users would have to evaluate different factors to determine what information to delete and when it should be deleted.[113] Under OUDEA, however, this would be a one-time cost because OUDEA would make it easy to automatically delete content in bulk using the expiration setting options. For example, a Twitter user could preset all tweets to delete every five days. The user-cost associated with such a decision would involve only the time and effort required to make the initial deletion setting.

B. Users Have Control Through Privacy and View Settings

Some may argue that OUDEA is unnecessary because users already control their information and reputation through current website privacy and view settings. However, privacy and view settings alone

and (4) place the mouse over the message and click delete. *Deleting a Tweet*, *supra* note 24. The site notes that "[d]eleted [t]weets sometimes hang out in Twitter search, they will clear with time" but fails to provide any time frame. *Id.* The only option is to delete tweets one-by-one; Twitter "do[es] not provide a way to bulk-delete [t]weets." *Id.*

110. *See, e.g.*, *Basic Privacy Settings & Tools*, FACEBOOK, http://www.facebook.com/help/325807937506242 (last visited Apr. 6, 2013).

111. *See, e.g.*, *About Public and Protected Tweets*, TWITTER, https://support.twitter.com/articles/14016-about-public-and-protected-tweets (last visited Apr. 6, 2013) (notifying users that the default Twitter account setting for tweets is public); Colin Zick, *On or Off? Setting Defaults for Privacy Online*, SECURITY, PRIVACY & L. (June 15, 2012), http://www.securityprivacyandthelaw.com/2012/06/articles/retail-customer-information-sp/on-or-off-setting-defaults-for-privacy-online/ (describing how "Do Not Track" is set as "off" by default for Microsoft's Mozilla FireFox Internet browser and that users do not know that they are being "tracked" in the first place); Ian Ayers & Robert Gertner, *Filling Gaps in Incomplete Contracts: An Economic Theory of Default Rules* 99 YALE L.J. 87, 91 (1989) (discussing general theories of default rules).

112. Such costs include learning how to use the settings and learning about the technology offered, arguably a low cost because OUDEA mandates that websites make this easy; decision-making costs in determining what content to delete and when to delete it; and time costs associated with setting time limits.

113. Different factors that users may consider include: (1) the circumstances under which they are publishing content; (2) whether they want the content to remain forever or to be permanently erased after a certain period of time; (3) who can view the content; (4) risk of potential harm posed by the content; and (5) value of the content and potential benefits to the user for allowing the content to remain on the Internet.

are not enough because not all websites provide the same level of protection.[114] OUDEA would give users more control over their information by mandating that websites provide a deletion setting, rather than letting the websites make that choice themselves.[115] OUDEA would also provide users with the power and right to decide when they want their content to be deleted.[116]

C. Mandated Deletion Technology is Unnecessary When Websites can Delete User Content Themselves

Some may claim that because websites already have the ability to delete, mandated deletion technology is unnecessary. This criticism ignores that self-interested website operators have much more incentive to resist deletion than purveyors of independent expiration technology. Website operators profit from gathering, storing, aggregating, and selling user information and the social media business model is to collect and use information without limitation.[117] Whereas entities that offer expiration technology do not rely on the retention and unfettered use of user data—they rely on its deletion.[118] Further, the expiration technology that OUDEA requires would eliminate the time and effort websites expend on data removal and eliminate waiting periods that users are currently required to accept because the technol-

114. *Compare Protecting and Unprotecting Your Tweets,* TWITTER, https://support.twitter.com/groups/31-twitter-basics/topics/107-my-profile-account-settings/articles/20169886-how-to-protect-and-unprotect-your-tweets (last visited Mar. 12, 2013) (detailing user-account privacy options where users may opt to protect tweets from the default public view, however once the setting is changed back to unprotected all previous protected tweets become public. Upon protection selection, only user-approved followers can view that user's tweets and the user can prevent users from re-tweeting his or her tweets through other setting selections), *with Basic Privacy Settings & Tools*, FACEBOOK, http://www.facebook.com/help/325807937506242/ (last visited Mar. 12, 2013), *and Advanced Privacy Controls*, FACEBOOK, http://www.facebook.com/help/466544860022370/ (last visited Mar. 12, 2013) (describing privacy settings for Timeline viewers including: content sharing, limiting public visibility of posts, tags, photographs, and profile picture and information, and user control over removing other user's tags of that user in photographs and posts).

115. *See supra* Part II.A.

116. *See supra* Part II.A.

117. *See* Gillette, *supra* note 21 (describing the present business model of social media websites, which is to acquire as much user data as possible to sell to marketers).

118. *See Privacy Policy*, BURN NOTE, https://burnnote.com/privacy (explaining that "it is Burn Note's policy to expunge your data as soon as possible after it has served its purpose") (last visited Apr. 6, 2013); G.F., *This Message Will Self-destruct*, THE ECONOMIST BABBAGE BLOG (Aug. 5, 2012, 11:14 AM), http://www.economist.com/blogs/babbage/2012/08/internet-security (describing the development of self-deleting technology and services in response to a "backlash against the culture of constant sharing and archiving that Facebook, Twitter and other social networks encourage").

ogy would independently and automatically delete the information.[119] OUDEA would also provide users with notice and a remedy to ensure that when a website says data will be deleted they either fulfill that promise or face the consequences.[120]

D. OUDEA Demands Too Much of Websites

Website operators may argue that OUDEA demands too much by requiring them to implement independent deletion technology, create a setting application, and provide users with notice. However, websites frequently delete and remove data from their servers and offer deletion options to their users.[121] Since a majority of companies and service providers presently offer deletion technology and control, OUDEA's data deletion concept is not radically new.

Twitter, for example, notifies its users that they retain the rights to any content they submit, but that through the act of posting content through Twitter's service, the user grants Twitter a "worldwide, non-exclusive, royalty-free license" to do just about anything with his or her tweets.[122] Since Twitter acknowledges that users retain the rights to any content they submit, it would be consistent with Twitter's offering to allow users to choose whether they want Twitter to have that content forever. It would not be impossible for a website to offer technology that automatically deletes content,[123] especially because technology like TigerText is available and can be implemented into the website system[124]. It would save the website time and money be-

119. *See, e.g.*, Cheng, *supra* note 23 (noting that Facebook takes up to thirty days to permanently remove photos from its server).

120. *See supra* Part II.A.

121. *See supra* note 107.

122. *Terms of Service*, TWITTER, https://twitter.com/tos (last visited Apr. 11, 2012).

123. Facebook already offers this service through its Poke mobile phone application. *See* Heather Kelly, *Facebook Releases Poke App for Self-destructing Messages*, CNN (Dec. 22, 2012), http://www.cnn.com/2012/12/21/tech/social-media/facebook-poke-app (describing Facebook's Poke mobile phone application, which allows users to send time-limited disappearing messages to their Facebook friends). *But see* Jim Edwards, *Facebook's Self-deleting Pokes Can Be Resurrected 90 Days Later*, BUS. INSIDER (Jan. 2, 2013, 5:10 PM), http://www.businessinsider.com/facebooks-poke-photos-last-up-to-90-days-2013-1 (describing that *disappear* does not mean *delete*, that deletion is not permanent until 90 days after the expiration, and that the content can be retrieved from logs and backup storage).

124. *See supra* note 77 (describing TigerText); Tomio Geron, *TigerText Secures (and Erases) Your Text Messages*, FORBES (June 15, 2011), http://www.forbes.com/sites/tomiogeron/2011/06/15/tigertext-secures-and-erases-your-text-messages/ (stating that the consumer service of TigerText is free and that TigerText offers a paid enterprise service where companies can control the settings of the messages its employees send). Geron explains "the site has had traction among hospitals, which need to comply with HIPAA laws about how information about patients can be distributed among hospital employees. The

cause some user-generated content would automatically delete in bulk without action by the website. The technology could be programmed to notify the user directly and automatically when specific content has been deleted,[125] which would require no separate action by the website.[126] For these reasons, what OUDEA would require from websites is not overly burdensome.

In December 2012, Facebook introduced a mobile phone application called Facebook Poke which allows Facebook users to send photos, messages, pokes, and ten-second videos to Facebook friends which expire and disappear after a designated period of time ranging from one to ten seconds.[127] Although Facebook is in charge of the deletion process of the data, which is not ideal for the reasons mentioned above, such an offering illustrates that Facebook is willing to provide users with data-self-destructing options.[128]

E. No Feasible Way to Determine if Content has Actually Been Deleted

Even though websites subject to OUDEA would be required to provide users with expiration technology, a risk remains that such websites could disable the technology to keep copies for themselves. Websites might also alter the technology in order to allow them to keep data longer than the user permitted. Website operators may even argue that they need the content to improve their services and better tailor their marketing. OUDEA's accountability requirements should reduce non-compliance risks. OUDEA would punish websites that copy content designated to be deleted or that keep content longer than directed through fines and the user private right of action for damages.[129] Despite the fact that the expiration settings may not be one hundred percent foolproof because of technical glitches and websites finding ways to circumvent the technology, significant privacy and control value stems from providing users content control through a delete-by-default option.

service could also be used by bankers, lawyers, corporate board members, or others with regulatory requirements." *Id.*

125. TigerText does this. *See supra* note 77 and accompanying text.

126. *See supra* notes 74, 76.

127. *See* Edwards, *supra* note 123.

128. *Id.*

129. *See supra* Part II.A.

F. Harm in the Loss of Valuable Information

Some critics fear that auto-expire laws would cause valuable information to be lost forever. For example, Peter Fleischer, Google's global privacy counsel, has expressed the view that, "on one extreme, government-mandated auto-expire laws would be as sensible as burning down a library every 5 years."[130] Some people emphasize the value of a complete history of people's interactions on the Internet.[131] When a library burns down, public information that society determines is valuable, because it is worth housing in a library, are lost. However, libraries do not store daily correspondence, photographs, and web histories of everyday people because those are not as valuable to society. Fleischer's analogy does not apply to the destruction of all user-generated information. It applies only to valuable information. Fleischer cannot possibly believe that deleting *all* types of information would lead to a loss of vast amounts of value.[132] Just because the Internet provides an accessible, permanent record of all interactions does not mean that the Internet would lose substantial value if some user-generated information expired. While OUDEA's delete-by-default approach would retain less than complete information about a user's interactions on the Internet and his or her user-generated content, the loss is minimal when compared to the costs of permanent digital memory.[133]

G. First Amendment Concerns

Web companies, such as Google and Facebook, argue that privacy today is being used to justify censorship.[134] Because OUDEA would

130. Fleischer, *supra* note 102.

131. *See* Matt Raymond, *How Tweet It Is!: Library Acquires Entire Twitter Archive*, LIBRARY OF CONG. BLOG (Apr. 14, 2010), http://blogs.loc.gov/loc/2010/04/how-tweet-it-is-library-acquires-entire-twitter-archive/ (noting that, for experimental purposes, the Library of Congress digitally archives every public tweet ever made since Twitter's inception in March, 2006); Debby Bruck, *Library Of Congress a Generation Twitter Time Capsule of Public Tweets*, HUBPAGES BLOG (May 2, 2012), http://debbybruck.hubpages.com/hub/Library-Of-Congress-A-Generation-Twitter-Time-Capsule-of-Public-Tweets (describing the collection of tweets).

132. Fleischer, *supra* note 102 (stating that "in the real world, [Fleischer] suspect[s] that an auto-expire functionality (regardless of whether it was optional or mandatory) would provide little real-world practical privacy protections for users, but it would result in the lose [sic] of vast amounts of data and all the benefits that data can hold").

133. *See supra* Parts I.B & II.A (OUDEA §2(b) & (d)).

134. *See, e.g.*, Fleischer, *supra* note 102; Zach Whittaker, *Google's European Conundrum: When Does Privacy Mean Censorship?*, CNET (Mar. 1, 2013), http://news.cnet.com/8301-1009_3-57571966-83/googles-european-conundrum-when-does-privacy-mean-censorship/ (describing web companies' (like Google, Facebook, and Twitter) positions on privacy and

permit only users to delete self-generated content,[135] censorship concerns are not implicated by OUDEA to any significant extent. OUDEA would encourage retroactive self-censorship, not censorship of others. Through its data expiration technology mandate, OUDEA recognizes the users' right to be forgotten and gives control without infringing on others' free speech rights. Under OUDEA, deleted data would most likely be highly personal, harmful, or embarrassing information specific to the user. OUDEA would not hinder people's ability to disclose truthful information about other individuals, such as repeating an embarrassing comment made by a friend. Depending on the technology, OUDEA could place a burden on the re-posting party to find another way to "copy" the material, like transcribing the comment word-for-word. Unlike the European right to be forgotten, which would apply to third party copies of harmful postings about users,[136] OUDEA serves user control interests without affecting free speech interests.[137]

H. Potential for Abuse

Some individuals are concerned about the potential for abuse of data expiration technology.[138] Permanent deletion technology may thwart law enforcement efforts[139] and decrease online security when child pornographers, predators, and other criminals use the technology to carry out their crimes and harmful behavior. While these are serious concerns, the potential for misuse by a few should not preclude Congress from granting users a beneficial control over their online content.

---

the right to be forgotten as directly conflicting with free speech and as forms of censorship).

135. *See supra* Part II.A.

136. *Proposed Data Protection Regulation*, *supra* note 96, at 51.

137. *See supra* Part II.A.

138. *See, e.g.*, Filterthree, *The Potential Dangers of Tiger Text*, YOUTUBE (May 12, 2011), http://www.youtube.com/watch?v=Xl6s63x058c&feature=related (discussing lawmakers' concerns with TigerText technology and the associated risks of abuse by potential and past criminals).

139. *See* Gerry Smith, *Wickr Security App Makes Messages and Photos Self-Destruct*, HUFFINGTON POST (June 27, 2012), http://www.huffingtonpost.com/2012/06/27/wickr-security-app-messages-self-destruct_n_1631675.html (describing that the mobile phone application, Wickr, "uses technology to ensure that messages cannot be recovered, not even by law enforcement officers, who can acquire subpoenas to compel wireless providers or Internet service providers to turn over suspects' data as evidence").

I. Too Cumbersome for Users

Some may argue that users will find it too difficult to decide what information they should delete and when. It may also be difficult to know what information users will want to have available at a future date. Even if deletion time frames are tentative, readjusting takes some effort and the time costs of "re-thinking" or "re-planning" may add up so that users might find making adjustments inconvenient to them and ignore the delete function altogether. While a multitude of factors[140] will affect any one decision pertaining to a piece of content, this does not invalidate the need for more user control. Even though some users may never employ the expiration technology that OUDEA would require websites to provide,[141] other users may find the control feasible, helpful, and easy to apply to the content they generate online.[142] The benefits that OUDEA would provide to users—through expiration settings, notice, reporting, sanctions, and redress—are invaluable.[143] Just because some might not take advantage of OUDEA's benefits does not mean that they should not be available to those who would.

IV. Hurdles to OUDEA's Passage—Politics and Powerful Lobbyists

Some may oppose OUDEA's delete-by-default approach by raising post-9/11 national security and terrorism threat concerns.[144] They may argue that social networks should permanently preserve all user-generated content, especially because "[a]bout 90 [percent] of organized terrorism on the [I]nternet is being carried out through social media."[145]

140. *See supra* note 113 (listing factors that users will consider when deciding whether to delete a piece of content).

141. *See supra* Part II.A.

142. Services already exist which allow Internet users to set similar settings for content they generate online. *See* Gilbert, *supra* note 91 (describing Burn Note self-deleting messaging service).

143. *See supra* Part II.A.

144. *See* G.F., *supra* note 118 (noting that the justice department and security agencies are concerned that such data destruction tools and anonymous and secure communication mediums "might be useful to criminals and or terrorists").

145. *Terrorist Groups Recruiting Through Social Media, Facebook, Twitter Also Used to Gather Intelligence*, CBC NEWS (Jan. 10, 2012), http://www.cbc.ca/news/technology/story/2012/01/10/tech-terrorist-social-media.html; *see also* Emil Protalinski, *After Denouncing SOPA and PIPA, How Can Facebook Support CISPA?*, ZDNET (Apr. 12, 2012), http://www.zdnet.com/blog/facebook/after-denouncing-sopa-and-pipa-how-can-facebook-support-cispa/11700 (describing Facebook's support for the proposed bill called "Cyber Intelligence Sharing

Social network operators appeal to Congress to pass laws that further their interests.[146] For example, Facebook established a political action committee in 2011 and reported giving $193,000 to lawmakers during that year.[147] Facebook spent a record $960,000 on lobbying during the second quarter of 2012.[148] The more politicians and lawmakers rely on social media, the more influence social network companies may have on the passage of laws like OUDEA. Given increased lobbying by social networks and Internet giants[149] and the amount of money they spend to influence lawmakers on specific issues that affect their businesses and profitability,[150] such parties would likely mount significant opposition to OUDEA if they viewed it as a threat to their interests. However, because Facebook already offers its users data-destruction services through its mobile phone application Facebook Poke,[151] it is possible that, at least from Facebook, OUDEA would face little resistance.

Congress may also hesitate to pass OUDEA-type legislation if websites like Facebook and Twitter generate user opposition. If legislation like OUDEA lacks user support or if users openly protest against it, lawmakers may not support its passage.[152]

---

and Protection Act [(CISPA)], where provisions of the bill would allow private companies to voluntarily share user information and data with the U.S. government and vice versa if the information is relevant to a "cyber threat"); CISPA, H.R. 3523, 112th Cong. (2012), *available at* http://www.gpo.gov/fdsys/pkg/BILLS-112hr3523rfs/pdf/BILLS-112hr3523rfs.pdf.

146. Cecilia Kang, *Web Giants Launch Lobbying Group*, WASH. POST (Sept. 19, 2012), http://www.washingtonpost.com/business/economy/web-giants-launch-lobbying-group/2012/09/19/8cbb0bfc-0297-11e2-91e7-2962c74e7738_story.html.

147. David Saleh Rauf, *Facebook Lobbying Sets Record in Q2*, POLITICO (July 7, 2012), http://www.politico.com/news/stories/0712/78804.html.

148. *Id.*

149. *See, e.g.*, Kang, *supra* note 146 (describing a new lobbying association launched by Facebook, Google, Amazon, and Yahoo "to counter efforts by federal regulators to saddle their industry with new rules").

150. *Id.*

151. *See supra* note 124.

152. The Stop Online Piracy Act ("SOPA"), the Protect IP Act ("PIPA"), and the January 18, 2012 protests illustrate how vocal opposition to legislation that may threaten social networks' interests can affect political support for legislation passage. Before January 18, 2012, 48 members of the Senate and 32 members of the House supported the bills, while six members of the Senate and 25 members of the House opposed them. After January 18, 2012, Senate support decreased by eleven and House support by six, where opposition increased in the Senate by sixteen and by 70 in the House. While SOPA and PIPA were viewed as threats to individual privacy and freedom on the web, some could view data-destruction in a similarly threatening way. *Stop SOPA: How People and Social Media Changed Lawmakers' Minds (INFOGRAPHIC)*, HUFFINGTON POST (Jan. 20, 2012), http://www.huffingtonpost.com/2012/01/20/stop-sopa-congress-changed-their-mind-on-sopa_n_1219759.html.

Politicians and lawmakers have become Internet users as it becomes the primary means of communicating with their constituents.[153] They generate content on the Internet and social networks to strengthen their campaigns,[154] agendas, and to increase political communications. Websites like Facebook and Twitter are valuable communication and advertising channels for political campaigns.[155] As one article noted, "[m]embers of Congress are using Facebook in different ways—from buying ads to conducting town halls—as a vehicle to boost engagement with constituents and expand their support online."[156] Thus, as users themselves, Congressmen and women may support OUDEA because they post content to the Internet, which may come back to haunt them later.[157]

Conclusion

Users should demand increased control over their user-generated content and challenge the permanent digital memory norm. Time for change is ripe. Today, users' opinions are widely broadcasted through

153. *See, e.g.*, *United States President Barack Obama's Facebook Page*, FACEBOOK, https://www.facebook.com/barackobama (last visited Apr. 6, 2013); *New York City Mayor Mike Bloomberg's Facebook Page*, FACEBOOK, https://www.facebook.com/mikebloomberg (last visited Apr. 6, 2013); *California Senator Dianne Feinstein's Facebook Page*, FACEBOOK, https://www.facebook.com/SenatorFeinstein (last visited Apr. 6, 2013); *Washington State Senator Maria Cantwell's Twitter Page*, TWITTER, https://twitter.com/CantwellPress (last visited Apr. 6, 2013); *California Governor Jerry Brown's Twitter Page*, TWITTER, https://twitter.com/JerryBrownGov (last visited Apr. 6, 2013).

154. *See, e.g.*, Matthew Fraser & Soumitra Dutta, *Barack Obama and the Facebook Election*, U.S. NEWS (Nov. 19, 2008), http://www.usnews.com/opinion/articles/2008/11/19/barack-obama-and-the-facebook-election (describing President Barack Obama's use of social networking sites to connect directly with voters).

155. *Id.*

156. Jennifer Moire, *Update: Facebook Spent a Record $1.35 Million Lobbying During 2011*, ALLFACEBOOK (Jan. 21, 2012, 8:13 PM), http://allfacebook.com/facebook-spent-record-1-35-million-lobbying-2011_b74619.

157. *See, e.g.*, Bianca Bosker, *The Twitter Typo That Exposed Anthony Weiner*, HUFFINGTON POST (June 7, 2011), http://www.huffingtonpost.com/2011/06/07/anthony-weiner-twitter-dm_n_872590.html (discussing Rep. Anthony Weiner (D-NY)'s accidental posting of a lewd picture to Twitter, which caused him to resign). Three house staffers for Democratic Congressman Rick Larsen, of Washington State's second district, were fired after months of tweets that described on-the-job drinking and public insults of Congressman Larsen. Some of the tweets read: "Dear taxpayers—I hope you don't mind that I'm watching YouTube clips of Nirvana at my government job. Thanks, you're the best."; "My coworker just took a shot of Jack crouching behind my desk. We have unabashedly given up on just about all things work related."; and "I really like DC, but I could have used another day away. The silver lining is that I don't have to see my idiot boss." *Tweets from Congressional Staffers Describe On-Job Drinking in Office of Congressman Larsen*, NW DAILY MARKER (Dec. 8, 2011), http://www.nwdailymarker.com/2011/12/tweets-from-congressional-staffers-describe-on-job-drinking-in-office-of-congressman-larsen/.

various social media and Internet-news forums[158] and traditional media outlets.[159] These demands gain the attention of websites,[160] as well as others involved in social media communities.[161] Websites take user input seriously[162] and users have the potential to change a website's position on its terms of service and offerings.[163] Given this ability, users must express concern for increased control over their content through discussions on blogs and social media forums. User demands should be heard off the Internet as well by urging lawmakers to pass a law solidifying these demands. Users should also call on privacy advocate groups for support.[164] Users should not be content with the present take-it-or-leave-it situation. User support for legislation, such as OUDEA, would provide users with more control over their data, including determining how long their content should exist on the Internet. It is imperative that users pressure lawmakers to support OUDEA-type legislation. Congress must recognize that, at present, users have inadequate bargaining power to effect change from these large Internet companies, and therefore, legislative backing is

158. *See, e.g.*, *User Backlash Proves to be a Challenge for Facebook*, BUS. STANDARD (Apr. 11, 2013), http://www.business-standard.com/article/technology/user-backlash-proves-to-be-a-challenge-for-facebook-11301040v]0018_1.html [hereinafter *User Backlash*] (noting that user backlash and opposition creates obstacles for Facebook's sales growth).

159. *See, e.g.*, *Instagram Takes Back Policy Change, Says Users' Photos Won't Appear in Ads*, FOX NEWS (Dec. 18, 2012), http://www.foxnews.com/tech/2012/12/18/instagram-takes-back-policy-change-says-users-photos-wont-appear-in-ads/ (reporting that Instagram's terms of service change, which would allow the company to use its users' photographs in advertisements, upset users).

160. *See* Kevin Systtom, *Thank you, and We're Listening*, INSTAGRAM BLOG, http://blog.instagram.com/post/38252135408/thank-you-and-were-listening (last visited Apr. 7 2013).

161. *See* Jenna Wortham, *Facebook Responds to Anger Over Proposed Instagram Changes*, N.Y. TIMES (Dec. 18, 2012), http://www.nytimes.com/2012/12/19/technology/facebook-responds-to-anger-over-proposed-instagram-changes.html (explaining that user outrage and concerns over Instagram terms of service changes surfaced on social media forums like Twitter and Instagram).

162. *See* Systtom, *supra* note 160.

163. *See* Wortham, *supra* note 161 (noting that Instagram would change terms of service because of user concerns); Francis Bea, *Instagram Fights Back, Releases Performance Stats for the First Time*, DIGITAL TRENDS (Jan. 17, 2013), http://www.digitaltrends.com/social-media/instagram-fights-back-releases-performance-stats-for-the-first-time/ ("The Internet reacted and revolted in dismay when Instagram's terms and conditions suggested that its monetization scheme included owning the rights to its user's content and allow brands and advertisers access to it. Users shut down their accounts and celebrities fled. The uproar finally compelled Instagram to revert back to backpedal a bit [sic]. . . .").

164. *See, e.g.*, ELECTRONIC PRIVACY INFORMATION CENTER (EPIC), http://epic.org/privacy/privacy_resources_faq.html (last visited Apr. 7, 2013); ELECTRONIC FRONTIER FOUNDATION (EFF), https://www.eff.org/ (last visited Apr. 7, 2013).

essential. This Comment encourages users to increase awareness of the need, and their desire, to change the permanency default by demanding that Congress enact legislation like OUDEA.